

# Simultaneous communication in noisy channels

Amit Weinstein\*

## Abstract

A sender wishes to broadcast a message of length  $n$  over an alphabet to  $r$  users, where each user  $i$ ,  $1 \leq i \leq r$  should be able to receive one of  $m_i$  possible messages. The broadcast channel has noise for each of the users (possibly different noise for different users), who cannot distinguish between some pairs of letters. The vector  $(m_1, m_2, \dots, m_r)_{(n)}$  is said to be feasible if length  $n$  encoding and decoding schemes exist enabling every user to decode his message. A rate vector  $(R_1, R_2, \dots, R_r)$  is feasible if there exists a sequence of feasible vectors  $(m_1, m_2, \dots, m_r)_{(n)}$  such that  $R_i = \lim_{n \rightarrow \infty} \frac{\log_2 m_i}{n}$ , for all  $i$ .

We determine the feasible rate vectors for several different scenarios and investigate some of their properties. An interesting case discussed is when one user can only distinguish between all the letters in a subset of the alphabet. Tight restrictions on the feasible rate vectors for some specific noise types for the other users are provided. The simplest non-trivial cases of two users and alphabet of size three are fully characterized. To this end a more general previously known result, to which we sketch an alternative proof, is used.

This problem generalizes the study of the Shannon capacity of a graph, by considering more than a single user.

## 1 Introduction

A sender has to transmit messages to  $r$ -users, where the user number  $i$  should be able to receive any one of  $m_i$  messages. To this end, the sender broadcasts a message of length  $n$  over an alphabet  $\Sigma$  of size  $k$ . Each user  $i$  has a confusion graph  $G_i$  on the set of letters of  $\Sigma$ , where two letters  $a, b \in \Sigma$  are connected if and only if user  $i$  cannot distinguish between  $a$  and  $b$ . The sender and users can agree on a (deterministic) coding scheme. For each possible values  $a_i$  of the messages,  $1 \leq a_i \leq m_i$ , the scheme should enable the sender to transmit a string of length  $n$  over  $\Sigma$  so that each user  $i$  will be able to recover  $a_i$ . The vector of a scheme for length  $n$  messages is  $(m_1, m_2, \dots, m_r)$ . The rate vector of a sequence of schemes is the limit

$$\lim_{n \rightarrow \infty} \left( \frac{\log_2 m_1}{n}, \frac{\log_2 m_2}{n}, \dots, \frac{\log_2 m_r}{n} \right),$$

---

\*Blavatnik School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Email: amitw@tau.ac.il. Research supported in part by an ERC advanced grant.

assuming the limit exists for this sequence. Our objective is to study which vectors and which rate vectors are feasible for a given set of confusion graphs  $G_i$ . This seems to be difficult even for relatively small cases, and reveals some interesting phenomena. Note that this problem generalizes the problem of computing the *Shannon capacity* of a graph which was first considered by Shannon in [10]. In the case of a single user (i.e. a single confusion graph  $G$ ), the maximum feasible rate is precisely  $\log_2 c(G)$  where  $c(G)$  denotes the Shannon capacity of  $G$ .

Investigating the feasible rate vectors for a given set of confusion graphs raises another interesting question. What is the maximum capacity of the channel for all users together? The total capacity can be measured as the sum of rates for each user, which we refer to as the *total rate*. This sum encapsulates the usability of the channel.

The individual rates we consider in this paper are sometimes referred to as *private rates*. Similarly, there is an analogue question about the *common rate*, determining how much information could we use if we require all users to receive the same message. This question is outside the scope of our work, but for completeness we refer the reader to [5] for more information and results.

## 1.1 Initial Observations

The relation between the described problem and the Shannon capacity leads to the following upper bound on the users' rates and hence for the total rate as well.

**Proposition 1.** *Given  $r$  users whose confusion graphs are  $G_1, G_2, \dots, G_r$ , a feasible rate vector  $(R_1, R_2, \dots, R_r)$  must satisfy  $R_i \leq \log_2 c(G_i)$  for every  $1 \leq i \leq r$ , hence  $\sum_{i=1}^r R_i \leq \sum_{i=1}^r \log_2 c(G_i)$ .*

Although in practice we have several users, their total rate cannot exceed the possible rate of a single user who shares all their information. Given a set of confusion graphs  $G_1, \dots, G_r$ , let  $G = \cap_{i=1}^r G_i$  be the graph over the same alphabet  $\Sigma$ , where  $a, b \in \Sigma$  are connected in  $G$  if and only if they are connected in  $G_i$  for every  $i$ . The confusion graph  $G$  represents the information all users have together and therefore can bound their total rate as follows.

**Proposition 2.** *Given  $r$  users whose confusion graphs are  $G_1, G_2, \dots, G_r$ , any feasible rate vector  $(R_1, R_2, \dots, R_r)$  must satisfy  $\sum_{i=1}^r R_i \leq \log_2 c(\cap_{i=1}^r G_i)$ .*

An important simple property of the feasible rate vectors is *convexity*, which is often referred to as *time sharing*. Informally, the messages we broadcast can be shared between two or more broadcasting schemes, where each part corresponds to a different scheme. This property can be stated formally as follows.

**Proposition 3.** *Let  $G_1, G_2, \dots, G_r$  be the confusion graphs for  $r$  users. Given two feasible rate vectors  $\bar{R}, \bar{R}'$  and  $\alpha \in [0, 1]$ , the rate vector  $\alpha \bar{R} + (1 - \alpha) \bar{R}'$  is also feasible.*

*Proof.* Since both  $\bar{R}$  and  $\bar{R}'$  are feasible rate vectors, each has some corresponding encoding scheme. Our new encoding scheme would be to use the encoding scheme corresponding to  $\bar{R}$  in

the first  $\alpha n$  coordinates and the one corresponding to  $\overline{R}'$  in the remaining  $(1 - \alpha)n$  coordinates. The resulting rate vector is precisely  $\alpha \overline{R} + (1 - \alpha) \overline{R}'$ , as required.  $\square$

**Corollary 4.** *Let  $G_1, G_2, \dots, G_r$  be the confusion graphs for  $r$  users. Given  $x_1, x_2, \dots, x_r \in [0, 1]$  so that  $\sum_{i=1}^r x_i = 1$ , the rate vector  $(x_1 \cdot \log_2 c(G_1), \dots, x_r \cdot \log_2 c(G_r))$  is feasible.*

*Proof.* For every  $1 \leq i \leq r$ , the rate vector consisting of rate  $\log_2 c(G_i)$  for the  $i$ 'th user and zero rate for all other users is trivially feasible. The result thus follows by Proposition 3.  $\square$

## 1.2 Previous Results

The problem of simultaneous communication in noisy channels was previously studied in the theory of broadcast channels (see [3] and its references). For some scenarios, such as the one we will describe shortly, a full characterization of all feasible rate vectors was found (see [8] and [9]). This scenario is described here fully as it is used in some of our proofs and as we also provide a sketch for an alternative proof for it.

Let  $\Sigma_k = \{\sigma_1, \sigma_2, \dots, \sigma_k\}$  be an alphabet of size  $k$  and let  $G_1, G_2, \dots, G_r$  be the confusion graphs for the  $r$  users, where each confusion graph is a disjoint union of cliques. Given user  $i$ , one can view his noise as receiving  $y_i = f_i(x)$  whenever  $x$  is transmitted, where  $f_i(x) : \Sigma_k \mapsto \{1, 2, \dots, \ell_i\}$  is the index of the clique which  $x$  belongs to and  $\ell_i$  is the number of cliques in the  $i$ 'th user's confusion graph. Note that we consider isolated vertices as cliques of size one and hence  $f_i$  is well defined up to the order of the cliques.

**Definition 1.** *Given a probability distribution  $p$  over  $\Sigma_k$  and a subset of the users  $I \subseteq \{1, 2, \dots, r\}$ , let  $H_{(p)}(\{Y_i\}_{i \in I})$  be the binary entropy of the random variables  $\{Y_i\}_{i \in I}$  where  $Y_i = f_i(X)$  and  $X$  is the random variable distributed over  $\Sigma_k$  according to  $p$ .*

For each subset of the users  $I \subseteq \{1, 2, \dots, r\}$ , the alphabet  $\Sigma_k$  can be partitioned into  $s \leq k$  disjoint parts  $(A_1, \dots, A_s)$  according to what these users receive  $(\{f_i(x)\}_{i \in I})$ . These users cannot distinguish between different letters from the same part  $A_j$ , so their joint information when sending a letter  $X$  from  $\Sigma_k$  according to the probability distribution  $p$  can be computed as

$$H_{(p)}(\{Y_i\}_{i \in I}) = - \sum_{1 \leq j \leq s} \Pr[X \in A_j] \cdot \log_2 \Pr[X \in A_j] .$$

Therefore in a sense that will be made precise later, when using only messages in which the letters are distributed according to some distribution  $p$ , we expect no subset  $I$  of users to have total rate which exceeds  $H_{(p)}(\{Y_i\}_{i \in I})$ .

The following theorem, for which we sketch an alternative proof, provides the full characterization of all feasible rate vectors.

**Theorem 5** ([9]). *Let  $G_1, G_2, \dots, G_r$  be the confusion graphs for  $r$  users over the alphabet  $\Sigma_k = \{\sigma_1, \sigma_2, \dots, \sigma_k\}$ , where each confusion graph is a disjoint union of cliques. Using the notations and*

definitions above, a rate vector  $(R_1, R_2, \dots, R_r)$  is feasible if and only if there exists a probability distribution  $p = (p_1, \dots, p_k)$  over  $\Sigma_k$  so that for every subset  $I \subseteq \{1, 2, \dots, r\}$  of the users,

$$\sum_{i \in I} R_i \leq H_{(p)}(\{Y_i\}_{i \in I}).$$

An interesting special case of the above theorem is the symmetric dense scenario of  $r = k$  users, where the confusion graph  $G_i$  of user  $i$  is a clique over  $\Sigma_k - \{\sigma_i\}$ . In other words, user  $i$  only distinguishes the letter  $\sigma_i$  from all other letters. When decoding, the relevant information for user  $i$  is only the locations of  $\sigma_i$  in the transmitted message.

**Corollary 6.** *For every fixed  $k \geq 3$ ,  $(\frac{\log_2 k}{k}, \dots, \frac{\log_2 k}{k})$  is a feasible rate vector over the alphabet  $\Sigma_k = \{\sigma_1, \sigma_2, \dots, \sigma_k\}$ , when each confusion graph  $G_i$  is a clique on  $\Sigma_k - \{\sigma_i\}$ .*

Corollary 6 indicates the possible gain of encoding schemes for several users simultaneously. The total rate here is  $\log_2 k$ , whereas using convexity with encoding schemes for single users cannot exceed a total rate of 1 (as this is the maximum rate for each single user; the Shannon capacity  $c(G_i)$  is precisely 2 for each  $1 \leq i \leq k$ ). However, in some cases there is no such gain. Several examples are discussed in what follows.

### 1.3 Our Results

For simplicity we omit all floor and ceiling signs whenever these are not crucial.

Let  $\Sigma_k = \{\sigma_1, \sigma_2, \dots, \sigma_k\}$  be an alphabet of size  $k$  and let  $\Sigma_d = \{\sigma_1, \dots, \sigma_d\}$  denote the set of the first  $d$  letters of  $\Sigma_k$ , where  $2 \leq d \leq k$ . Consider the case where user 1 has a confusion graph

$$G_1 = (\Sigma_k, \{ab \mid a \in \Sigma_k \wedge b \in \Sigma_k - \Sigma_d\}),$$

meaning the complete graph over  $\Sigma_k$  minus a clique over  $\Sigma_d$ . The Shannon capacity of such graphs is easily shown to be  $c(G_1) = d$ , hence the maximum rate of user 1 is at most  $\log_2 d$ . The following results indicate, that for two different confusion graphs of user 2, nothing can be gained beyond convexity of single user encoding schemes. We need the following definition.

**Definition 2.** *A rate vector is optimal if no user can increase his rate while the other user maintains the same rate.*

Note that the total rate of such optimal rate vectors does not necessarily reach the maximum total rate possible.

**Theorem 7.** *In the scenario described above for  $2 \leq d \leq k$ , when user 2 has the empty confusion graph  $G_2 = (\Sigma_k, \emptyset)$ , the rate vectors  $(\alpha \log_2 d, (1 - \alpha) \log_2 k)$  for  $\alpha \in [0, 1]$  are optimal.*

**Theorem 8.** *In the scenario described above for  $2 \leq d \leq \frac{k+1}{2}$ , when user 2 has the complement confusion graph, that is*

$$G_2 = \overline{G_1} = (\Sigma_k, \{ab \mid a, b \in \Sigma_d\}),$$

*the rate vectors  $(\alpha \log_2 d, (1 - \alpha) \log_2(k - d + 1))$  for  $\alpha \in [0, 1]$  are optimal.*

Finally, we provide a full characterization of all feasible rate vectors for all scenarios containing two users and alphabet of size three (Propositions 15, 16 and 17).

## 1.4 Organization

The rest of the paper is organized as follows. In Section 2 we present a sketch of an alternative proof to the characterization of the feasible rate vectors for the first scenario, where each confusion graph is a union of disjoint cliques, (Theorem 5), and demonstrate how combining encoding schemes for many users can sometimes outperform convexity (Corollary 6). Section 3 deals with the second family of confusion graphs described above in which convexity yields the optimal rate vectors (Theorems 7 and 8). Combining these results, one can characterize all feasible rate vectors for all scenarios involving two users and alphabet of size three. In Section 4 we elaborate in more details on this analysis. The final Section 5 contains some concluding remarks and open problems.

## 2 Unions of disjoint cliques - outperforming convexity

We consider the case where the confusion graph of each user  $i$  is a disjoint union of cliques. This case is of special interest as a full description of all feasible rate vectors was known and it is deterministic in the sense that given the transmitted letter, we can transform it deterministically to the different symbols that each user receives. Moreover, choosing specific confusion graphs, it demonstrates how the maximum possible total rate can be achieved by combining schemes for many users (and only this way), even when the confusion graphs are nearly complete.

### 2.1 An alternative proof of Theorem 5 (sketch)

Let  $G_1, G_2, \dots, G_r$  be a set of confusion graphs for  $r$  users over the alphabet  $\Sigma_k$ , where each  $G_i$  is a disjoint union of cliques. Given a subset of the users  $I \subseteq [r]$  (where  $[r] = \{1, 2, \dots, r\}$ ), the following definition and Lemma connects between the possible number of messages to these users and their binary entropy, when restricted to a specific distribution of the messages

**Definition 3.** *Given a probability distribution  $p$  over  $\Sigma_k$  and a subset of the users  $I \subseteq [r]$ , let  $N_{(p)}(n; \{Y_i\}_{i \in I})$  denote the number of possible (different) messages for these users under the restriction that each message is originated in a length  $n$  message over  $\Sigma_k$  in which  $\sigma_i$  appears  $p_i n$  times.*

**Lemma 9.**

$$\frac{2^{H_{(p)}(\{Y_i\}_{i \in I})n}}{n^k} \leq N_{(p)}(n; \{Y_i\}_{i \in I}) \leq 2^{H_{(p)}(\{Y_i\}_{i \in I})n}.$$

The proof of Lemma 9 is a simple consequence of Stirling's formula, which is left to the reader.

*Upper bound.* Given a scheme of a fixed length  $n$  which realizes  $(m_1, m_2, \dots, m_r)$  messages for the  $r$  users, one can divide it into families according to the number of appearances of the letters

$\sigma_i$  in each message. As there are only  $k$  letters and all the messages are of length  $n$ , there are at most  $n^{k-1}$  different families. Given the probability  $p = (p_1, p_2, \dots, p_k)$  corresponding to the largest family, Lemma 9 therefore indicates that

$$\frac{\prod_{i \in [r]} m_i}{n^{k-1}} \leq N_{(p)}(n; \{Y_i\}_{i \in I}) \leq 2^{H_{(p)}(\{Y_i\}_{i \in I})n}.$$

Recall that  $R_i = \lim_{n \rightarrow \infty} \log_2 m_i / n$  and hence

$$\begin{aligned} \sum_{i \in I} R_i &= \lim_{n \rightarrow \infty} \sum_{i \in I} \frac{\log_2 m_i}{n} = \lim_{n \rightarrow \infty} \frac{\log_2 \prod_{i \in I} m_i}{n} \\ &\leq \lim_{n \rightarrow \infty} \frac{H_{(p)}(\{Y_i\}_{i \in I})n + (k-1) \log_2 n}{n} \\ &= H_{(p)}(\{Y_i\}_{i \in I}) \end{aligned}$$

as required.  $\square$

**Remark:** Formally, the popular probability distribution  $p = (p_1, p_2, \dots, p_r)$  depends on  $n$  but one can take a subsequence for which it converges to a single vector  $p$ , justifying the computation above. A similar argument can be used in the following lower bound proof, justifying it for any probability distribution, even one containing irrational probabilities.

**Remark:** Similar arguments are sometimes referred to as *type counting* and could be found, for example, in the book by Csiszár and Körner [4]. They also provide a proof for a claim similar to Lemma 9.

*Lower bound.* Let  $p = (p_1, \dots, p_k)$  be a probability distribution over  $\Sigma_k$  and fix  $(R_1, R_2, \dots, R_r)$  so that for any subset of the users  $I \subseteq [r]$ ,  $\sum_{i \in I} R_i \leq H_{(p)}(\{Y_i\}_{i \in I})$ . Given some large  $n$ , we set the number of messages  $m_i$  for each user  $i$  to be  $m_i = \frac{2^{R_i n}}{n^{k+2}}$  (which clearly satisfies  $\lim_{n \rightarrow \infty} \frac{\log_2 m_i}{n} = \lim_{n \rightarrow \infty} \frac{R_i n - (k+2) \log_2 n}{n} = R_i$ ). By Lemma 9, for every subset of the users  $I \subseteq [r]$ ,

$$\begin{aligned} \prod_{i \in I} m_i &= \prod_{i \in I} \frac{2^{R_i n}}{n^{k+2}} = \frac{2^{\sum_{i \in I} R_i n}}{n^{(k+2)|I|}} \\ &\leq \frac{2^{H_{(p)}(\{Y_i\}_{i \in I})n}}{n^{k+2}} \leq \frac{N_{(p)}(n; \{Y_i\}_{i \in I})}{n^2}. \end{aligned} \tag{1}$$

Our encoding scheme will use only messages in which the letters of  $\Sigma_k$  are distributed according to  $p$ . For each user  $i$  there are  $N_{(p)}(n; \{Y_i\})$  different messages that he can identify. We randomly divide them into  $m_i$  families  $\mathcal{F}_{i,1}, \dots, \mathcal{F}_{i,m_i}$ , where each family represents a different message for user  $i$ . When the message  $\bar{x} \in \Sigma_k^n$  is transmitted, user  $i$  receives  $\bar{y}_i = f_i(\bar{x}) = f_i(x_1) \cdots f_i(x_n)$  and decodes the message  $j$ , the single  $j \in [m_i]$  for which  $\bar{y}_i \in \mathcal{F}_{i,j}$ .

In order to complete the proof we show the described encoding scheme is valid for some selection of families  $\mathcal{F}_{i,j}$ . Such a scheme is valid if for every set of messages  $\{j_i \in [m_i]\}_{i \in [r]}$  there exists a message  $\bar{x}$  so that for every user  $i \in [r]$ ,  $\bar{y}_i \in \mathcal{F}_{i,j_i}$ .

Given fixed messages  $j_1, j_2, \dots, j_r$  for the  $r$  users, using the extended Janson inequality (c.f., e.g., [2], Chapter 8) and (1) one can show that the probability that there exists no valid message as required is less than  $\frac{1}{k^n}$ . As there are  $\prod_{i=1}^r m_i \leq k^n$  distinct choices for messages  $j_1, \dots, j_r$ , the assertion of Theorem 5 follows by the union bound.  $\square$

**Remark:** A full citation of the extended Janson inequality can be found in Appendix A, together with a more detailed description of how it is used here.

## 2.2 Proof of Corollary 6

This corollary of Theorem 5 is for the symmetric dense case where there are  $r = k$  users, and each user  $i$  distinguishes a single letter from all other letters. This simple case demonstrates how the maximum rate can be achieved only by mixing the messages for all the users. Since each confusion graph  $G_i$  is a clique on  $\Sigma_k - \{\sigma_i\}$ , the Shannon capacity of this graph is 2 and therefore the maximal rate for any single user is 1. However, the theorem shows that indeed a total rate of  $\log_2 k$  can be achieved, and obviously this is best possible.

Let  $k \geq 3$  be fixed. In order to prove the theorem, a probability distribution  $p$  is required so that for every subset of the users  $I \subseteq [r] = [k]$ ,

$$\sum_{i \in I} R_i = |I| \frac{\log_2 k}{k} \leq H_{(p)}(\{Y_i\}_{i \in I}). \quad (2)$$

Let us consider the uniform probability distribution  $p$ ,  $p_i = 1/k$  for every letter  $\sigma_i$ . When considering all users together, the random variables  $\{Y_i\}_{i \in [r]}$  indicate the exact letter  $x$  that was transmitted. Therefore, since the entropy is exactly  $\log_2 k$ ,  $H_{(p)}(\{Y_i\}_{i \in [r]}) = \log_2 k$  which indeed satisfies (2) as  $\sum_{i \in [r]} R_i = r \frac{\log_2 k}{k} = \log_2 k$ .

Given a subset of the users  $I \subset [r]$ , the random variables  $\{Y_i\}_{i \in I}$  indicate which letter  $x$  was transmitted if  $x = \sigma_i$  for  $i \in I$  or alternatively, that some other letter was transmitted. Hence its binary entropy satisfies

$$\begin{aligned} H_{(p)}(\{Y_i\}_{i \in I}) &= |I| \frac{\log_2 k}{k} + \frac{k - |I|}{k} \log_2 \frac{k}{k - |I|} \\ &> |I| \frac{\log_2 k}{k} = \sum_{i \in I} R_i \end{aligned}$$

thus (2) holds for every subset of the users  $I \subseteq [r]$ , as required.  $\square$

## 3 A clique minus a clique - convexity is everything

We consider the case where the confusion graph  $G_1$  of the first user is the complete graph on  $k$  vertices minus a clique on  $d$  vertices. We give an upper bound on the rate of the other user for both the empty confusion graph and for  $\overline{G}_1$ . In both cases, the results imply that optimal

encoding can be achieved by convexity, that is nothing can be gained by encoding the messages together. In order to prove Theorems 7 and 8, we need the following lemmas whose proofs are provided in Appendix B.

**Lemma 10.** *Given  $a, b \in \mathbb{N}$  s.t.  $2 \leq b \leq a$  and  $x_1 \geq x_2 \geq \dots \geq x_b \geq 0$ ,*

$$(a - b + 1)a^{\log_b x_b} + \sum_{i \in [b-1]} a^{\log_b x_i} \leq a^{\log_b \sum_{i \in [b]} x_i}.$$

**Remark:** Define here  $a^{\log_b 0} = 0$  hence we allow  $x_b$  to be 0.

**Lemma 11.** *Given  $2 \leq d \leq k \in \mathbb{N}$  and a set  $\mathcal{G} \subseteq \Sigma_k^n$ , we define  $\mathcal{G}' = \mathcal{G} \cap \Sigma_d^n$ . If  $\mathcal{G}$  is closed under replacing each  $\sigma_i$  with  $\sigma_j$  for any  $i > d$  and  $j \in [k]$ , then either  $|\mathcal{G}| = |\mathcal{G}'| = 0$  or*

$$\log_k |\mathcal{G}| \leq \log_d |\mathcal{G}'|.$$

**Lemma 12.** *Given  $2 \leq d \leq k \in \mathbb{N}$  s.t.  $d \leq \frac{k+1}{2}$  and a set  $\mathcal{G} \subseteq \Sigma_k^n$ , define  $\mathcal{G}' = \mathcal{G} \cap \Sigma_d^n$  and  $\mathcal{G}'' = \{f(g_1)f(g_2)\dots f(g_n) \mid g \in \mathcal{G}\}$  where  $f(\sigma_i) = \sigma_{\max\{i,d\}}$ . If  $\mathcal{G}$  is closed under replacing each  $\sigma_i$  with  $\sigma_j$  for any  $i > d$  and  $j \in [k]$ , then either  $|\mathcal{G}'| = |\mathcal{G}''| = 0$  or*

$$\log_{k-d+1} |\mathcal{G}''| \leq \log_d |\mathcal{G}'|.$$

**Remark:** The restriction of  $d$  is required as one can easily find an example where  $d = \lceil \frac{k+1}{2} \rceil$  for which the lemma does not hold (such examples are given in Appendix C).

*Proof of Theorem 7.* Let  $G_1, G_2$  be the confusion graphs as defined in the theorem and assume the rate of the first user is  $\alpha \log_2 d$  for some  $\alpha \in [0, 1]$ . The messages used can be divided into disjoint families  $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_{d^\alpha n}$  according to the message for the first user. Since the first user can only distinguish between the letters  $\sigma_i$  for  $i \in [d]$ , we can and will assume each such family  $\mathcal{F}_a$  is closed under replacing  $\sigma_i$  with  $\sigma_j$  for  $i > d$  and  $j \in [k]$ .

In order to prove this assumption is valid, it suffices to show user 1 can still distinguish between each of the families after these replacements. Notice that using this assumption might result in a different scheme, however, this shows that user 1 hasn't lost anything from this transition, while user 2 could possibly gain as we increased the size of each family (and he cannot lose since one could still use only the original families). Let  $\mathcal{G}_a$  denote the family  $\mathcal{F}_a$  after replacing  $\sigma_i$  with  $\sigma_j$  for  $i > d$  and  $j \in [k]$ . Assume by contradiction that there exist two families  $\mathcal{F}_a, \mathcal{F}_b$  and two vectors  $v_a \in \mathcal{G}_a, v_b \in \mathcal{G}_b$  so that user 1 can distinguish between  $\mathcal{F}_a$  and  $\mathcal{F}_b$  but cannot distinguish between  $v_a$  and  $v_b$ . By the definition of  $G_1$ , for every coordinate  $i \in [n]$ , either  $v_a[i] \notin \Sigma_d$  or  $v_b[i] \notin \Sigma_d$  or  $v_a[i] = v_b[i] \in \Sigma_d$  as otherwise user 1 would be able to distinguish between them (here  $v_x[i]$  denotes the  $i$ 'th letter in the vector  $v_x$ ). Since  $v_a \in \mathcal{G}_a$  and  $v_b \in \mathcal{G}_b$ , we know there exists  $u_a \in \mathcal{F}_a$  and  $u_b \in \mathcal{F}_b$  from which  $v_a$  and  $v_b$  can be derived by the replacements above. Therefore, for every coordinate  $i \in [n]$ , either  $u_a[i] \notin \Sigma_d$  or  $u_b[i] \notin \Sigma_d$  or  $u_a[i] = u_b[i] \in \Sigma_d$ . However, this is



in contradiction to the fact that user 1 was able to distinguish between  $\mathcal{F}_a$  and  $\mathcal{F}_b$  as he cannot distinguish between  $u_a$  and  $u_b$ .

Define  $\mathcal{F}'_a = \mathcal{F}_a \cap \Sigma_d^n$  for every  $\mathcal{F}_a$ . Since these families are pairwise disjoint, by an averaging argument there exists some message  $a$  for which  $|\mathcal{F}'_a| \leq d^{-\alpha n} \cdot d^n = d^{(1-\alpha)n}$ . By Lemma 11, for this specific message  $a$ ,  $|\mathcal{F}_a| \leq k^{(1-\alpha)n}$  which implies the rate of the second user is at most  $(1 - \alpha) \log_2 k$ .  $\square$

**Corollary 13.** *For the confusion graph  $G_1$  as above and any confusion graphs  $G_2, \dots, G_r$ , a feasible rate vector  $(\alpha \log_2 d, R_2, \dots, R_r)$  for  $\alpha \in [0, 1]$  must satisfy  $\sum_{i=2}^r R_i \leq (1 - \alpha) \log_2 k$ .*

*Proof of Theorem 8.* Let  $G_1, G_2$  be the confusion graphs as defined in the theorem. Note that the Shannon capacity  $c(G_2)$  is precisely  $k - d + 1$ , hence these rate vectors are feasible by Corollary 4 (as is also easy to see directly). Assume the rate of the first user is  $\alpha \log_2 d$  for some  $\alpha \in [0, 1]$ . The messages used can be divided into disjoint families  $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_{d^{\alpha n}}$  according to the message for the first user. Since the first user can only distinguish between the letters  $\sigma_i$  for  $i \in [d]$ , we can and will assume, as in the proof of Theorem 7, that each such family  $\mathcal{F}_a$  is closed under replacing  $\sigma_i$  with  $\sigma_j$  for  $i > d$  and  $j \in [k]$ .

Define  $\mathcal{F}'_a = \mathcal{F}_a \cap \Sigma_d^n$  for every  $\mathcal{F}_a$ . Since these families are pairwise disjoint, by an averaging argument there exists some message  $a$  for which  $|\mathcal{F}'_a| \leq d^{-\alpha n} \cdot d^n = d^{(1-\alpha)n}$ . Given the first user should receive the message  $a$ , the second user has at most  $|\mathcal{F}''_a| = |\{f(g_1)f(g_2) \cdots f(g_n) \mid g \in \mathcal{F}_a\}|$  different messages where  $f(\sigma_i) = \sigma_{\max\{i, d\}}$  (as the second user can only distinguish the locations of  $\sigma_i$  for  $i \in [k] - [d]$  and all other letters are indistinguishable for him). By Lemma 12, for this specific message  $a$ ,  $|\mathcal{F}''_a| \leq (k - d + 1)^{(1-\alpha)n}$  which implies the rate of the second user is at most  $(1 - \alpha) \log_2(k - d + 1)$ .  $\square$

**Corollary 14.** *For the confusion graph  $G_1$  as above and any confusion graphs  $G_2, \dots, G_r \supseteq \overline{G}_1$ , a feasible rate vector  $(\alpha \log_2 d, R_2, \dots, R_r)$  for  $\alpha \in [0, 1]$  must satisfy  $\sum_{i=2}^r R_i \leq (1 - \alpha) \log_2(k - d + 1)$ .*

## 4 Two users, three letters - the complete story

Two users and three letters is the smallest possible example of non-trivial scenario. Having only two letters result in each user either knowing everything or knowing nothing and obviously having a single user coincides with the Shannon capacity question. These smallest scenarios however already contain some interesting cases which we analyze using the previous results.

Let  $\Sigma = \{\sigma_0, \sigma_1, \sigma_2\}$  be our alphabet and let  $G_1, G_2$  be the confusion graphs of the two users correspondingly. If one of the confusion graphs is the complete graph, again it coincides with the Shannon capacity of a single graph (for the non-complete confusion graph). As stated earlier, there is a strong connection between the feasible rate vectors and the Shannon capacity of graphs. In the cases we are about to analyze, we use the fact that the Shannon capacity of every graph on 3 vertices which is neither the empty graph nor the clique, is precisely 2 (each such graph is

perfect, hence its Shannon capacity equals its independence number). By the symmetry between the users and the letters in the alphabet, it suffices to discuss only subset of the possible confusion graphs.

#### 4.1 Confusion graph with two edges

In this subsection we show that when the first confusion graph has two edges, then no scheme can outperform what follows from convexity.

**Proposition 15.** *Let  $G_1 = (\Sigma, \{\sigma_0\sigma_1, \sigma_0\sigma_2\})$ , meaning the first user only distinguishes between the letters  $\sigma_1$  and  $\sigma_2$ . For every  $G_2$ , the optimal rate vectors are given by Corollary 4, i.e.*

$$(\alpha \cdot \log_2 c(G_1), (1 - \alpha) \cdot \log_2 c(G_2))$$

for  $\alpha \in [0, 1]$  where  $\log_2 c(G_1) = 1$ .

**Remark:** Note that this matches the case of a clique minus a clique for the parameters  $k = 3$  and  $d = 2$  as denoted in previous sections, but here we do not limit the confusion graph of the second user.

*Proof.* The proof is divided into two parts, according to the intersection between the edges of  $G_1$  and  $G_2$ . In the first case where there is a non-empty intersection, the bound given by Proposition 2 yields a maximum total rate of  $\log_2 c(G_1 \cap G_2) = 1$ . Therefore, one could not hope for finding a feasible rate vector which is not of this form (assuming  $G_2$  is not the complete graph, these are all optimal rate vectors as they have a total rate of 1).

Let us assume there is no intersection between the two confusion graphs, meaning either  $G_2$  is the empty graph or  $G_2 = \overline{G_1}$ . These cases match Theorems 7 and 8 respectively which indeed yield the desired result.  $\square$

#### 4.2 The first confusion graph has a single edge

Throughout this section we denote  $H$  as the binary entropy function where given some probability distribution  $p_1, p_2, \dots, p_k, q$  (where  $q = 1 - \sum_{i=1}^k p_i$ ),

$$\begin{aligned} H(p_1, p_2, \dots, p_k, q) &= H(p_1, p_2, \dots, p_k) \\ &= - \sum_{i=1}^k p_i \log_2 p_i - q \log_2 q. \end{aligned}$$

**Proposition 16.** *Let  $G_1 = (\Sigma, \{\sigma_0\sigma_1\})$  and  $G_2 = (\Sigma, \{\sigma_0\sigma_2\})$ . The following rate vectors are optimal:*

- $(R_1, H(R_1))$  for  $R_1 \in [1/2, 2/3]$ .

- $(R_1, \log_2 3 - R_1)$  for  $R_1 \in [2/3, \log_2 3 - 2/3]$ .
- $(H(R_2), R_2)$  for  $R_2 \in [1/2, 2/3]$ .

**Remark:** By the proposition a rate vector  $(R_1, R_2)$  in the above case is feasible if and only if

1.  $R_1 \in [0, 1/2]$  and  $R_2 \in [0, 1]$  or
2.  $R_1 \in [1/2, 2/3]$  and  $R_2 \in [0, H(R_1)]$  or
3.  $R_1 \in [2/3, \log_2 3 - 2/3]$  and  $R_2 \in [0, \log_2 3 - R_1]$  or
4.  $R_1 \in [\log_2 3 - 2/3, 1]$  and  $R_2 \in [0, H^{-1}(R_1)]$ .

*Proof.* The scenario described above is a special case of Theorem 5. Given a probability distribution  $p = (p_0, p_1, p_2)$ ,  $y_1$  is distributed  $(p_0 + p_1, p_2)$ ,  $y_2$  is distributed  $(p_0 + p_2, p_1)$  and  $\{y_1, y_2\}$  is distributed according to  $p$ .

The uniform distribution  $p = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$  yields that the rate vectors  $(R_1, R_2)$  are feasible if  $R_1 + R_2 \leq \log_2 3$  and each  $R_i \leq H(2/3) = \log_2 3 - 2/3$ . This matches the second case described in the theorem, which is obviously optimal as one cannot hope to exceed a total rate of  $\log_2 3$ .

By symmetry, it suffices to analyze the first case of the theorem in order to complete the proof. Setting  $p_1$  to be some probability smaller than half bounds the rate of the second user by  $R_2 \leq H(p_1) = H(1 - p_1)$ . Moreover, the total rate  $R_1 + R_2$  is bounded by  $H(\frac{1-p_1}{2}, \frac{1-p_1}{2}, p_1) = H(p_1) + (1-p_1)$ . This shows that the rate vectors  $(R_1, H(R_1))$  are feasible as  $R_1 = 1-p_1 \leq H(\frac{1-p_1}{2})$  for  $p_1 \in [0, 1/2]$  (indeed equality holds for  $p_1 = 0$  and since  $H'(x) = \log_2(1-x) - \log_2 x < 2$  for  $x \in [1/4, 1/2]$ , or equivalently  $H'(\frac{1-p_1}{2}) > -1$  for  $p_1 \in [0, 1/2]$ , this holds for every  $p_1 \in [0, 1/2]$  as well). Moreover, these rate vectors are also optimal as the bound for the total rate  $H(p_1) + (1-p_1)$  decreases while  $p_1$  increases in the section  $[1/3, 1/2]$  (using  $H'(x) < 1$  for  $x \in [1/3, 1/2]$ ).  $\square$

**Remark:** Although the rate vector  $(1, 1/2)$  is feasible, the vector  $(2^n, 2)$  is not feasible. If user 1 needs to be able to receive  $2^n$  distinct messages, one of them has to be encoded by  $(\sigma_2, \sigma_2, \dots, \sigma_2)$ . But this has to be transmitted independently of the message of the second user, showing there is no  $(2^n, 2)$ -scheme.

**Proposition 17.** Let  $G_1 = (\Sigma, \{\sigma_0 \sigma_1\})$  and  $G_2$  be the empty graph. The following rate vectors are optimal:

- $(R_1, \log_2 3 - R_1)$  for  $R_1 \in [0, H(2/3)]$ .
- $(H(R_2), R_2)$  for  $R_2 \in [1/2, 2/3]$ .

**Remark:** By the proposition a rate vector  $(R_1, R_2)$  in the above case is feasible if and only if

1.  $R_1 \in [0, \log_2 3 - 2/3]$  and  $R_2 \in [0, \log_2 3 - R_1]$  or

2.  $R_1 \in [\log_2 3 - 2/3, 1]$  and  $R_2 \in [0, H^{-1}(R_1)]$ .

*Proof.* Our problem is monotone in the following sense. Removing an edge from one of the confusion graphs can only improve the feasible rate vectors. Therefore in our case, the lower bound of  $(H(R_2), R_2)$  for  $R_2 \in [1/2, 2/3]$  we achieved when both confusion graphs had a single edge can be applied here. Showing these rate vectors are also optimal will complete the proof as we have the trivial upper bound of  $\log_2 3$  on the total rate, and by combining convexity with the fact that the rate vectors  $(H(2/3), 2/3)$  and  $(0, \log_2 3)$  are feasible, we conclude that all other required rate vectors are achieved.

Our problem is a special case of Theorem 5. Note that in the proof of Proposition 16 we showed an upper bound for the rates  $(R_1, H(R_1))$  which only depended on the second user. Assuming the second user has rate of  $H(R_1)$  already bounds the total rate by  $H(R_1) + R_1$ . Similarly in our case, assuming the first user has rate of  $H(R_2)$  for  $R_2 \in [1/2, 2/3]$  bounds the total rate of the two users together by  $H(R_2) + R_2$ .  $\square$

## 5 Conclusions and open problems

In this work we have studied the notion of simultaneous communication in a noisy channel where the channel's noise may differ for each of the users. The goal is to find, for a given set of confusion graphs which represent the noise for each of the users, which rate vectors (or alternatively vectors) are feasible. As in the Shannon capacity of a channel, we care about the average rate per letter when the length of the messages tends to infinity.

Our work demonstrates basic lower and upper bounds for the general case. A simple yet useful tool in understanding the feasible rate vectors is the convexity property which is described in Proposition 3. We saw several examples where convexity and basic encoding schemes (derived from the Shannon capacity of the confusion graphs) are optimal. On the other hand, there are examples where much more can be gained by mixing the encoding for several users. The case in which every graph is a disjoint union of cliques is fully understood, and so is the case of 2 users and alphabet of size 3. Many other cases remain open.

We conclude with several open problems it would be interesting to solve.

- The lower and upper bounds for the maximum total rate given in this paper apply combinatorial and probabilistic techniques. It would be interesting to find stronger bounds which possibly extend the algebraic and geometric bounds known for the Shannon capacity, such as the bounds given by Lovász in [7], Hamers [6] or Alon [1].
- In the non-symmetric case where we have a user whose confusion graph is a clique over  $k$  letters minus a clique over  $d$  letters and the other user's confusion graph is its complement, it would be interesting to know if Theorem 8 still holds for  $d > \frac{k+1}{2}$ . Since Lemma 12 does not hold for such  $d$ , a different approach must be used.

- It seems interesting to study graphs  $G$  for which the maximum total rate is as small as possible using  $G$  and  $\overline{G}$  as the two confusion graphs for two users. In such a case, the upper bound of the Shannon capacity of the intersection (Proposition 2) does not help as the two graphs are disjoint. However, by Theorem 1.1 of [1], we know there exist graphs  $G$  on  $k$  vertices for which both  $c(G)$  and  $c(\overline{G})$  are at most  $e^{O(\sqrt{\log k \log \log k})}$ . For such a graph, the upper bound in Proposition 1 of the maximum total rate yields  $O(\sqrt{\log k \log \log k})$  which is far less than the trivial upper bound of  $\log_2 k$ .
- Most of the encoding schemes considered in this paper use randomness and therefore are not given explicitly. As a result, the encoding and decoding schemes are not efficient. Finding explicit and efficient encoding and decoding schemes for the scenarios described in the paper remains open.

## Acknowledgment

I am grateful to Alon Orlitsky and Ofer Shayevitz for helpful discussions. I am especially thankful to Noga Alon for his dedication, guidance and support throughout this research.

## References

- [1] N. Alon, *The Shannon capacity of a union*, Combinatorica 18 (1998), 301-310.
- [2] N. Alon and J. Spencer, *The Probabilistic Method, Third Edition*, Wiley 2008.
- [3] T. M. Cover, *Comments on broadcast channels*, IEEE Trans. Inform. Theory, vol. 44, pp. 2524-2530, Oct. 1998.
- [4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press 1981.
- [5] L. Gargano, J. Körner and U. Vaccaro, *Capacities: From Information Theory to Extremal Set Theory*, Journal of Combinatorial Theory, Series A 68, 296-316 (1994).
- [6] W. Haemers, *An upper bound for the Shannon capacity of a graph*, Colloq. Math. Soc. János Bolyai 25, Algebraic Methods in Graph Theory, Szeged, Hungary (1978), 267-272.
- [7] L. Lovász, *On the Shannon capacity of a graph*, IEEE Trans. Inform. Theory 25 (1979), 17.
- [8] K. Marton, *The capacity region of deterministic broadcast channels*, in Trans. Int. Symp. Inform. Theory (Paris-Cachan, France, 1977).
- [9] M. S. Pinsker, *Capacity of noiseless broadcast channels*, Probl. Pered. Inform., vol. 14, no. 2, pp. 283-284, Apr.-June 1978; translated in Probl. Inform. Transm., pp. 97-102, Apr.-June 1978.

- [10] C. E. Shannon, *The zero error capacity of a noisy channel*, IRE Trans. Inform. Theory 2 (1956), 819.

## A The extended Janson inequality and its application in Theorem 5

Below is the full citation of the extended Janson inequality, followed by its application in the lower bound proof of Theorem 5.

**Theorem 18** (Janson). *Let  $S$  be a set, for each  $s \in S$  let  $p_s$  be a real  $0 \leq p_s \leq 1$ . Let  $R$  be a random subset of  $S$  obtained by selecting each  $s \in S$ , randomly and independently, to lie in  $R$  with probability  $p_s$ . Let  $A_i, i \in I$  be a family of subsets of  $S$ . For each  $i \in I$ , let  $B_i$  be the event that  $A_i \subset R$ . Let  $\mu = \sum_{i \in I} \text{Prob}[B_i]$  be the expected number of events  $B_i$  that occur. Define  $\Delta = \sum \text{Prob}[B_i \wedge B_j]$ , where the sum ranges over all ordered pairs  $i, j \in I, i \neq j$  such that  $A_i \cap A_j \neq \emptyset$ . Then the probability that none of the events  $B_i$  occurs is at most  $e^{-\mu + \Delta/2}$ . If the further assumption that  $\Delta > \mu$  holds, this probability can also be bounded by  $e^{-\mu^2/2\Delta}$ .*

Given the process defined in the lower bound proof of Theorem 5, we fix messages  $j_1, j_2, \dots, j_r$  for the  $r$  users. Consider the  $r$ -uniform  $r$ -bipartite hypergraph whose classes of vertices are  $\mathcal{F}_{i,j_i}$ ,  $1 \leq i \leq r$ . Each edge represents a consistent message, i.e. for every message  $\bar{x} \in \Sigma_k^n$  there exists an edge  $\{\bar{y}_i \in \mathcal{F}_{i,j_i}\}_{i \in [r]}$  if indeed for every  $i \in [r]$ ,  $\bar{y}_i = f_i(\bar{x}) \in \mathcal{F}_{i,j_i}$ . Existence of some edge in the hypergraph indicates that this set of messages can be transmitted as required.

Using the notations of Theorem 18, our set  $S$  is the union of all possible messages  $f_i(\bar{x})$  for each user  $i$  and for  $\bar{x} \in \Sigma_k^n$  which is distributed according to  $p$ . The probability of each element is  $1/m_i$  for the relevant user  $i$ . The sets  $A_i$  represent all the consistent messages  $\{f_i(\bar{x})\}_{i \in [r]}$  where again,  $\bar{x} \in \Sigma_k^n$  and is distributed according to  $p$ .

By Theorem 18 the probability that there exists no valid message as required is at most  $e^{-\mu^2/2\Delta}$ . One can now verify that indeed, as defined here,  $\mu$  and  $\Delta$  satisfy  $e^{-\mu^2/2\Delta} \leq e^{-n^2/2^{k+1}} < \frac{1}{k^n}$ .

## B Proofs of Lemmas 10, 11 and 12

*Proof of Lemma 10.* When  $x_1 = x_2 = \dots = x_b$  equality holds as

$$\begin{aligned} (a - b + 1)a^{\log_b x_b} + \sum_{i \in [b-1]} a^{\log_b x_i} &= a \cdot a^{\log_b x_b} \\ &= a^{1 + \log_b x_b} = a^{\log_b b \cdot x_b} = a^{\log_b \sum_{i \in [b]} x_i}. \end{aligned}$$

In order to complete the proof, it suffices to show that the partial derivatives  $\frac{\partial}{\partial x_i}$  are smaller on the left hand side than those on the right hand side for any  $i \in [b-1]$ , regardless of the values  $\{x_i\}$ . Given a fixed  $i \in [b-1]$ , the derivative of the left hand side is  $\frac{\partial}{\partial x_i} a^{\log_b x_i} = \frac{\partial}{\partial x_i} x_i^{\log_b a} =$

$\log_b a \cdot x_i^{\log_b a - 1}$ . On the other hand, the derivative of the right hand side is  $\log_b a \cdot (\sum_{i \in [b]} x_i)^{\log_b a - 1}$  which is at least as big.  $\square$

*Proof of Lemma 11.* We apply induction on  $n$ . For  $n = 1$ , if  $\mathcal{G}' = \mathcal{G}$  the inequality holds as  $k \geq d$  (or both sets are empty). Otherwise there exists  $\sigma_i \in \mathcal{G}$  for  $i > d$ , hence  $|\mathcal{G}| = |\Sigma| = k$  and  $|\mathcal{G}'| = d$  for which equality holds.

Assuming the lemma holds for any  $n' < n$  we prove it for  $n$ . Define  $\mathcal{G}_i = \{g_1 g_2 \dots g_{n-1} \mid g \in \mathcal{G} \wedge g_n = \sigma_i\}$  and  $\mathcal{G}'_i = \mathcal{G}_i \cap \Sigma_d^{n-1}$  for every  $i \in [k]$ . Note that  $\mathcal{G}'_i \subseteq \mathcal{G}'_j$  and hence  $|\mathcal{G}'_i| \leq |\mathcal{G}'_j|$  for every  $i > d$  and  $j \in [d]$  (since  $\mathcal{G}$  is closed under replacing  $\sigma_i$  with  $\sigma_j$  for  $i > d$  and  $j \in [k]$ ). In particular, this is true for  $m \in [d]$  so that  $|\mathcal{G}'_m| = \min_{j \in [d]} |\mathcal{G}'_j|$ . Therefore, by the induction hypothesis and Lemma 10 with  $a = k$  and  $b = d$ ,

$$\begin{aligned}
|\mathcal{G}| &= \sum_{i \in [k]} |\mathcal{G}_i| \\
&\leq \sum_{i \in [k]} k^{\log_d |\mathcal{G}'_i|} \\
&\leq (k - d) k^{\log_d |\mathcal{G}'_m|} + \sum_{i \in [d]} k^{\log_d |\mathcal{G}'_i|} \\
&\leq (k - d + 1) k^{\log_d |\mathcal{G}'_m|} + \sum_{i \in [d] - \{m\}} k^{\log_d |\mathcal{G}'_i|} \\
&\leq k^{\log_d \sum_{i \in [d]} |\mathcal{G}'_i|} = k^{\log_d |\mathcal{G}'|}
\end{aligned}$$

completing the proof.  $\square$

*Proof of Lemma 12.* Again we apply induction on  $n$ . For  $n = 1$ , if  $\mathcal{G}' = \mathcal{G}$  we have no  $\sigma_i \in \mathcal{G}$  for  $i > d$  and the inequality holds as  $|\mathcal{G}''| = 1$  or both sets are empty. Otherwise there exists  $\sigma_i \in \mathcal{G}$  for  $i > d$ , hence  $|\mathcal{G}''| = k - d + 1$  and  $|\mathcal{G}'| = d$  for which equality holds.

Assuming the lemma holds for any  $n' < n$  we prove it for  $n$ . Extending the previous definitions of  $\mathcal{G}_i$  and  $\mathcal{G}'_i$ , let  $\mathcal{G}''_i = \{f(g_1)f(g_2)\dots f(g_{n-1}) \mid g \in \mathcal{G}_i\}$  for every  $i \in [k]$ . Note that  $\mathcal{G}''_i \subseteq \mathcal{G}''_j$  and hence  $|\mathcal{G}''_i| \leq |\mathcal{G}''_j|$  for every  $i > d$  and  $j \in [k]$  (since  $\mathcal{G}$  is closed under replacing  $\sigma_i$  with  $\sigma_j$  for  $i > d$  and  $j \in [k]$ ). Similarly,  $|\mathcal{G}''_i| \leq |\cap_{j \in [d]} \mathcal{G}''_j|$  for all  $i > d$ . Therefore,

$$\begin{aligned}
|\cup_{j \in [d]} \mathcal{G}''_j| &\leq \sum_{j \in [d]} |\mathcal{G}''_j| - (d - 1) \cdot |\cap_{j \in [d]} \mathcal{G}''_j| \\
&\leq \sum_{j \in [d]} |\mathcal{G}''_j| - (d - 1) \cdot \max_{i \in [k] - [d]} |\mathcal{G}''_i| \\
&\leq \sum_{j \in [d]} |\mathcal{G}''_j| - \frac{d - 1}{k - d} \sum_{i \in [k] - [d]} |\mathcal{G}''_i|.
\end{aligned}$$

As before,  $|\mathcal{G}'_i| \leq |\mathcal{G}'_m|$  for every  $i > d$  and  $m \in [d]$  so that  $|\mathcal{G}'_m| = \min_{j \in [d]} |\mathcal{G}'_j|$ . Therefore, by the induction hypothesis

$$\begin{aligned} \sum_{i \in [k] - [d]} |\mathcal{G}''_i| &\leq \sum_{i \in [k] - [d]} (k - d + 1)^{\log_d |\mathcal{G}'_i|} \\ &\leq (k - d)(k - d + 1)^{\log_d |\mathcal{G}'_m|}. \end{aligned}$$

By Lemma 10 with  $a = k - d + 1$  and  $b = d$  (which indeed satisfies  $2 \leq b \leq a$  as  $d \leq (k + 1)/2$ ),

$$\begin{aligned} |\mathcal{G}''| &= \sum_{i \in [k] - [d]} |\mathcal{G}''_i| + |\cup_{j \in [d]} \mathcal{G}''_j| \\ &\leq \frac{(k - d) - (d - 1)}{k - d} \sum_{i \in [k] - [d]} |\mathcal{G}''_i| + \sum_{j \in [d]} |\mathcal{G}''_j| \\ &\leq \frac{k - 2d + 1}{k - d} (k - d)(k - d + 1)^{\log_d |\mathcal{G}'_m|} \\ &\quad + \sum_{j \in [d]} (k - d + 1)^{\log_d |\mathcal{G}'_j|} \\ &= (k - 2d + 2)(k - d + 1)^{\log_d |\mathcal{G}'_m|} \\ &\quad + \sum_{j \in [d] - \{m\}} (k - d + 1)^{\log_d |\mathcal{G}'_j|} \\ &\leq (k - d + 1)^{\log_d \sum_{j \in [d]} |\mathcal{G}'_j|} = (k - d + 1)^{\log_d |\mathcal{G}'|} \end{aligned}$$

completing the proof.  $\square$

## C An example in which Lemma 12 does not hold when $d > \frac{k+1}{2}$

Let  $d = 3$ ,  $k = 4$  and  $n = 2$  where indeed  $d > \frac{k+1}{2} = 2.5$ . Define

$$\begin{aligned} \mathcal{G} &= \{(\sigma_1, \sigma_1), (\sigma_1, \sigma_2), (\sigma_1, \sigma_3), (\sigma_1, \sigma_4), \\ &\quad (\sigma_2, \sigma_1), (\sigma_3, \sigma_1), (\sigma_4, \sigma_1)\} \end{aligned}$$

which can also be viewed as  $\{(\sigma_1, \sigma_4), (\sigma_4, \sigma_1)\}$  after replacing  $\sigma_4$  with every  $\sigma \in \Sigma_4$  (as  $\mathcal{G}$  has to be closed under these replacements). By the definitions of the lemma,

$$\begin{aligned} \mathcal{G}' &= \{(\sigma_1, \sigma_1), (\sigma_1, \sigma_2), (\sigma_1, \sigma_3), (\sigma_2, \sigma_1), (\sigma_3, \sigma_1)\}, \\ \mathcal{G}'' &= \{(\sigma_3, \sigma_3), (\sigma_3, \sigma_4), (\sigma_4, \sigma_3)\} \end{aligned}$$

and therefore the lemma does not hold as

$$\log_{k-d+1} |\mathcal{G}''| = \log_2 3 > \log_3 5 = \log_d |\mathcal{G}'|.$$

The same example can be used with larger parameters, for instance with  $k = 100$  and  $d = 51$  (which is the minimal  $d$  for which  $d > \frac{k+1}{2}$ ). With these parameters,  $|\mathcal{G}'| = 2d - 1 = 101$  and  $|\mathcal{G}''| = 2(k - d + 1) - 1 = 99$  and indeed  $\log_{k-d+1} |\mathcal{G}''| = \log_{50} 99 > \log_{51} 101 = \log_d |\mathcal{G}'|$ .